
Willkommen
in der Computeria Wallisellen

Passwörter

Ein Vortrag über Passwörter und deren Verwaltung

Themen

- Passwörter
  - > Definition Passwort (PW)
  - > Authentifizierungsmethoden
- Bedrohungen
  - > Die wichtigsten Bedrohungen für Privatanwender
  - > Was tun im Schadenfall?
- Sichere Passwörter
  - > Generierung von sicheren PW
  - > Umgang mit PW
- PW Verwaltung
  - >Anforderung an ein PW-Verwaltungsprogramm
  - >Funktionen an einem PW-Verwaltungsprogramm
  - >Sonderfälle

❖.Passwort: Begriff

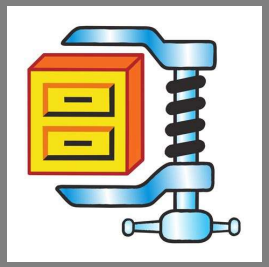
Nach Wikipedia:

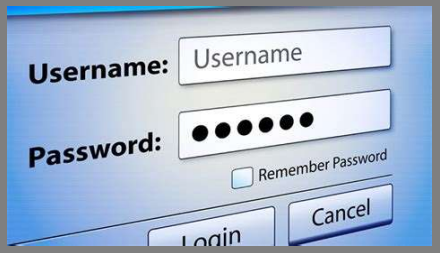
- Ein Passwort, Kennwort, auch Passphrase, Schlüsselwort, Codewort (auch Kodewort), Losung, Losungswort dient zur Authentifizierung.
- Eine Persönliche Identifikationsnummer (PIN) ist ein Passwort, das in der Regel ausschließlich aus Ziffern besteht.
- Basis ist ein Vertrag mit dem Dienstanbieter, der eingeschränkt Zugang bietet. Verantwortung ist in den AGB definiert !

Die Authentizität des sich so Ausweisenden bleibt nur höchstens so lange gewahrt, wie das Passwort geheim bleibt, das heißt, es Dritten nicht bekannt ist.

Quelle: https://de.wikipedia.org/wiki/Passwort

❖.Passwort: Nutzen / Authentisierungsverfahren





Verfahren:

>PIN

>User ID/ Passwort

>Karte / Passwort

>Multifaktoren Authentisierung

>Chipkarte

>Biometrische Daten

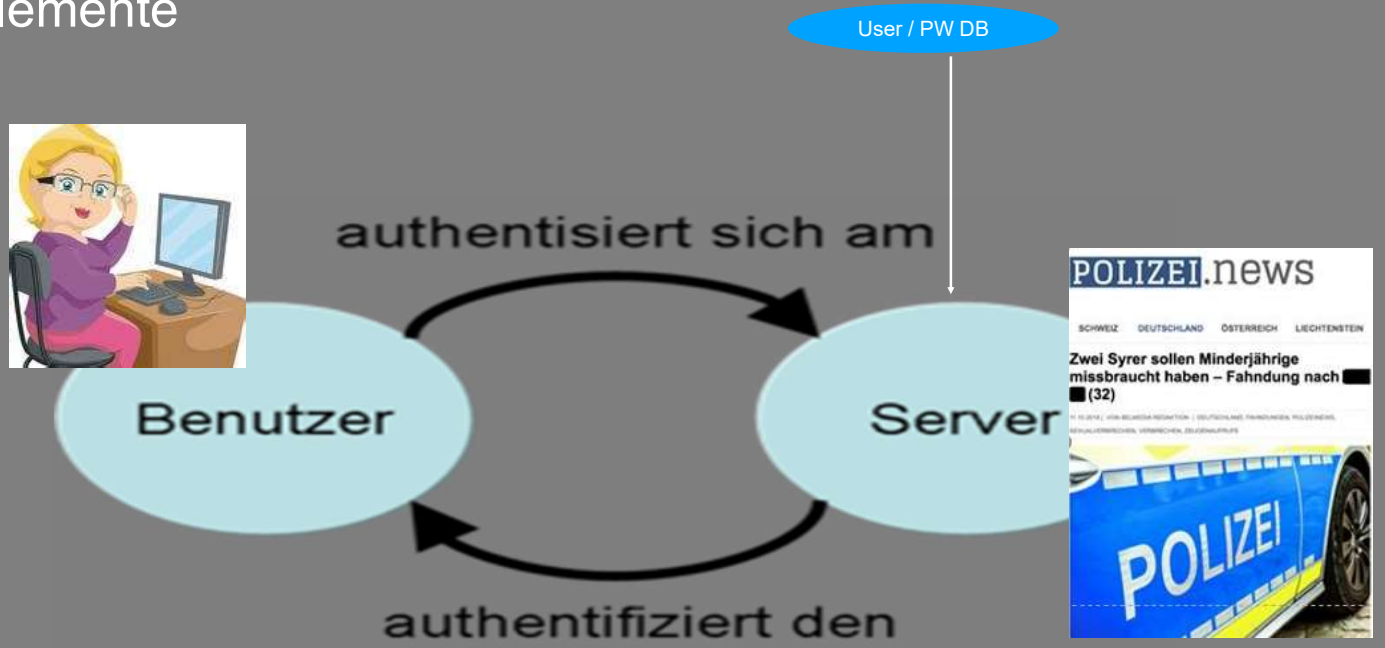
>Zertifikat

>SecureID

Quelle: https://de.wikipedia.org/wiki/Passwort

❖.Passwort: Authentifizierung

Identifikationsmerkmale:
Vertrags-ID / User-ID
Passwort
Zusätzliche Sicherheitselemente

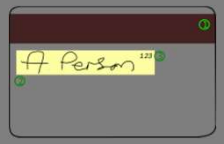


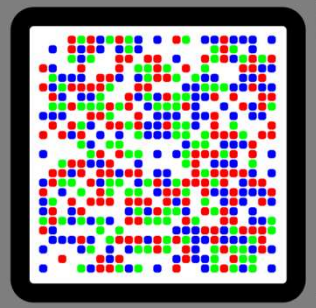
Quelle: https://de.wikipedia.org/wiki/Passwort

❖.Passwort: 2/Multi-faktoren Authentifizierung

Definition:

Die Zwei-Faktor-Authentisierung (2FA), häufig auch als *Zwei-Faktor-Authentifizierung* bezeichnet, bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).





Quelle: Vortrag Computeria, sicher bezahlen

❖.Passwort: Alternative Authentifizierungen

Spracherkennung

Chip Card

Fingerabdruck

Iris scanning

Dongle

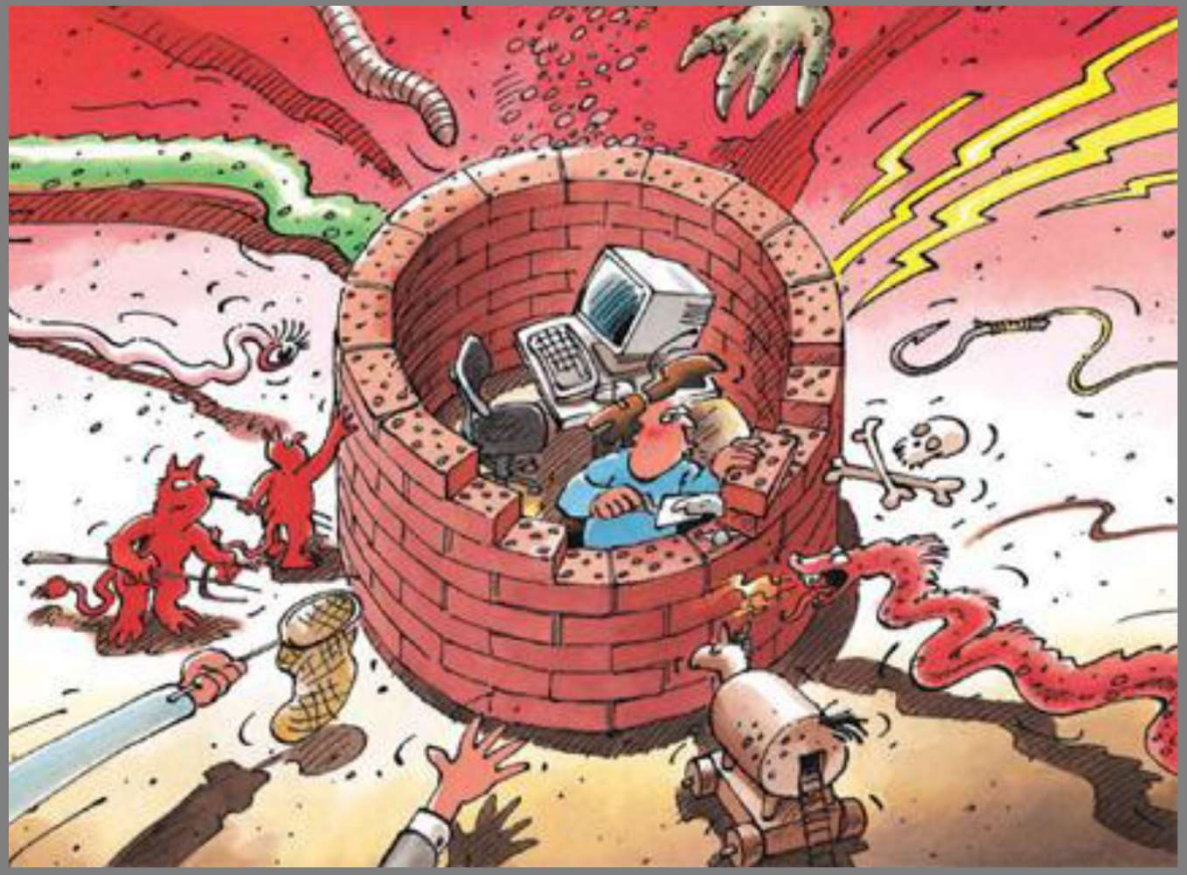
Gesichtserkennung

Quelle: https://de.wikipedia.org/wiki/Passwort

❖.Passwort:

Fragen?

❖.Bedrohungen: Cyberkriminalität



Die 5 wichtigsten Bedrohungen

- DDos Angriffe
- Phishing-Betrug
- Identitätsdiebstahl
- Exploit-Kits
- Ransomware

Ziele

- Betrug
- Erpressung
- Missbrauch
- Spionage
- Vorteil

Quelle: https://de.wikipedia.org/wiki/Passwort

❖.Bedrohungen: Definitionen

Ddos Angriffe (Distributed Denial-of-Service)
werden von Botnets ausgeführt. Ziel ist es Systeme durch Overload zum Absturz zu bringen.

Phishing-Betrug
Das Wort Phishing setzt sich aus den englischen Wörtern «Password», «Harvesting» und «Fishing» zusammen. Massenweise Versand von E-Mails mit Links zu bösartigen Websiten oder Anhänge mit bösartiger Software.

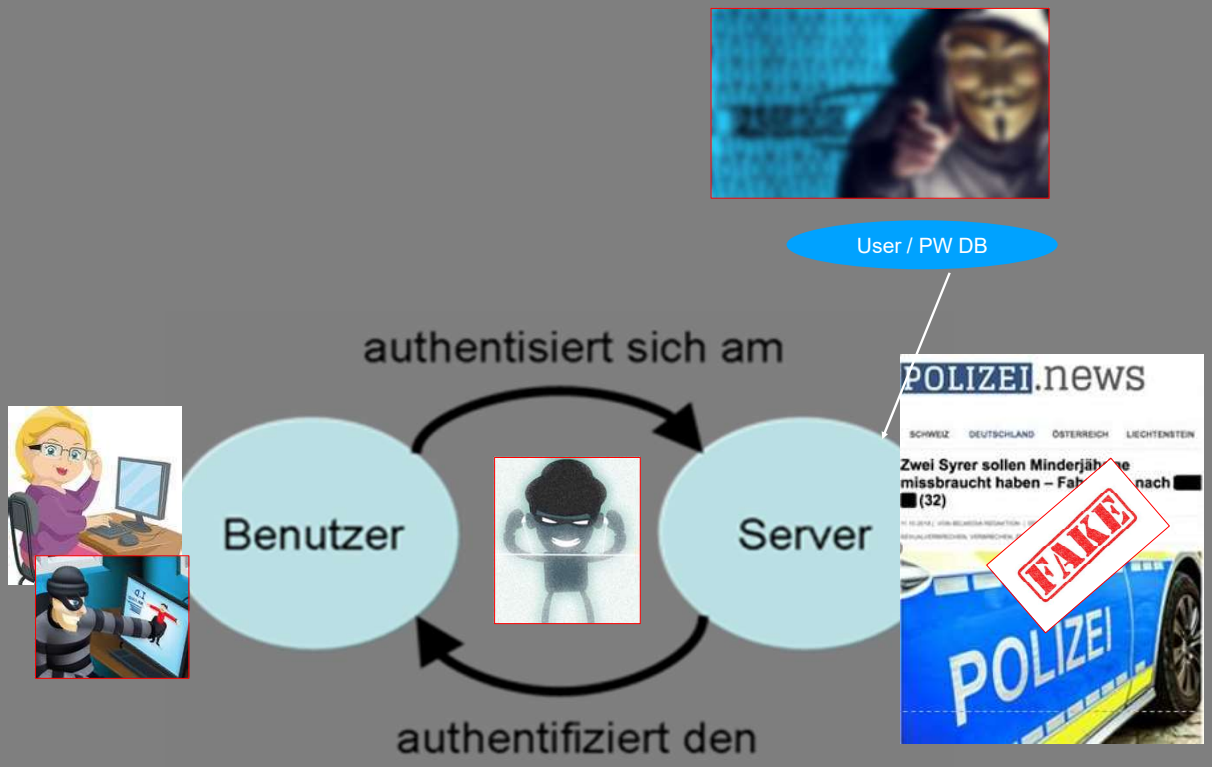
Identitätsdiebstahl
z.B. Skimming, Social Engineering, Mail-/Web Phishing, Brute-Force Angriff.

Exploit-Kits
Software die Fehler und Sicherheitsmängel auf Computer ausnutzen.

Ransomware
Ransomware ist eine bösartige Software, die das Opfer von ihrem Computer absperrt oder den Zugriff auf die gespeicherten Dateien der Festplatte blockiert.

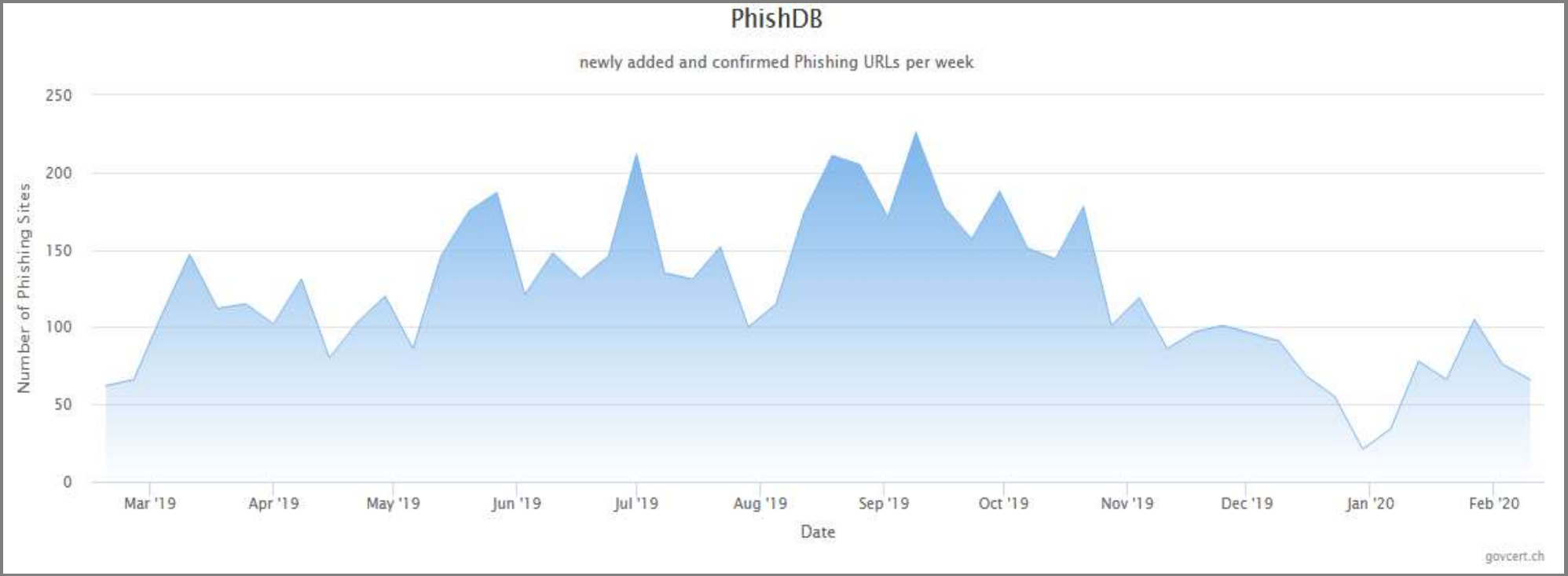
Quelle: Bitkom Research

❖.Bedrohungen: Wer greift wo an?



Quelle: Bitkom Research

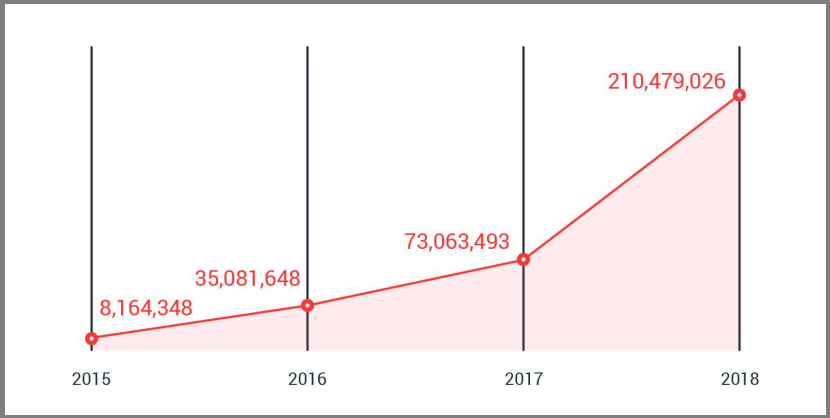
❖.Bedrohungen: Statistik über Phishing

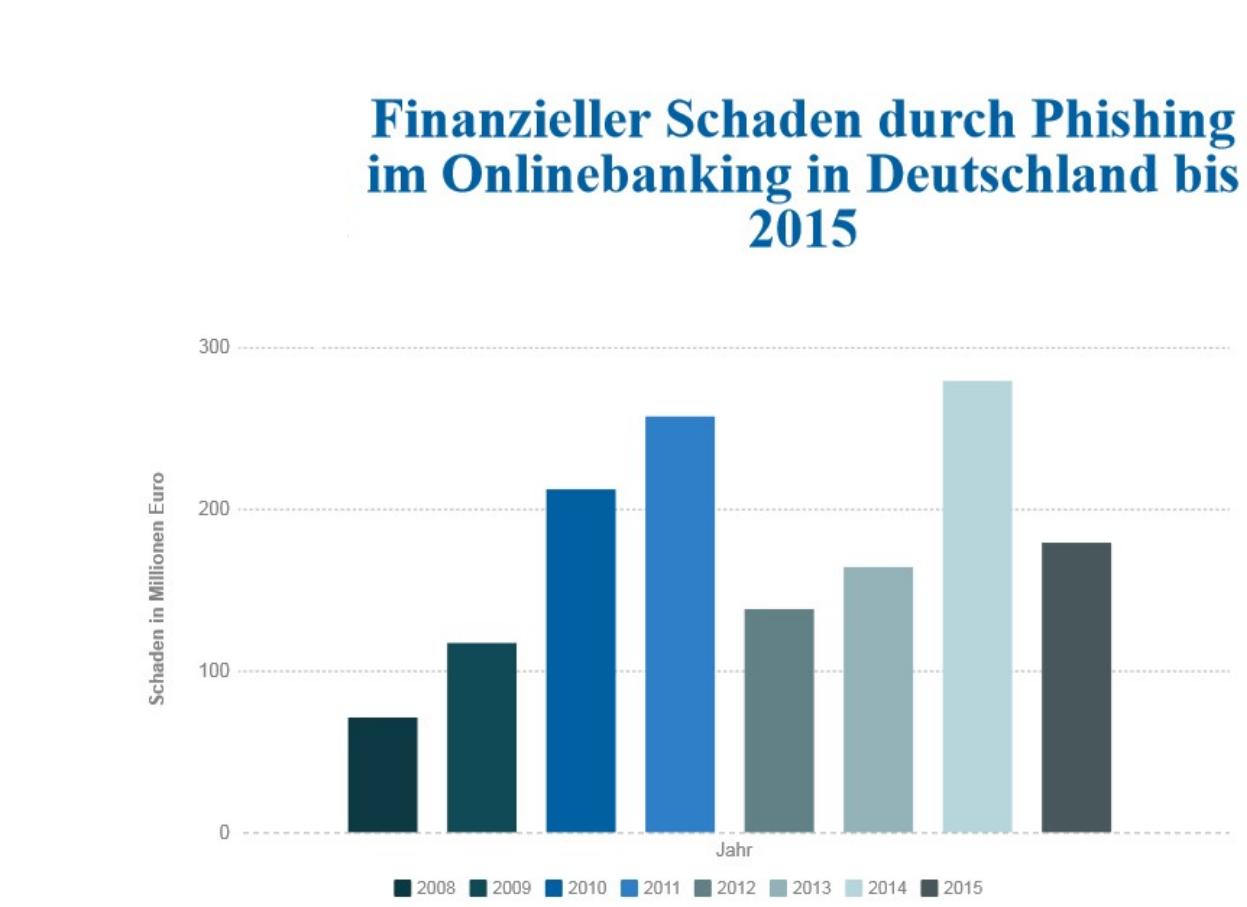


Im 1.Halbe Jahr 2019 sind 2521 Phishing fälle an Melani gemeldet worden (Cyberkriminalität)
in den letzten zwölf Monaten (2019) 371‘498 Hacking vom eigenen Profil auf sozialen Netzwerken oder vom E-Mail-Konto
In den letzten 12 Monate (Febr.2020) 2‘982‘638 Erhalt von betrügerischen Nachrichten (Phishing)

Quelle: Melani

❖.Bedrohungen: Statistik Phishing II





Quelle: internet

❖.Bedrohungen: Wie funktioniert E-Mail & Web-Site Phishing

Kein seriöser Dienstleister würde seine Kunden jemals per Mailnachricht oder Telefon zur Angabe von Passwörtern oder Kreditkartendaten auffordern.

Quelle: https://unsicherheitsblog.de/tag/phishing

❖.Bedrohungen: Wie funktioniert Phishing

https://www.youtube.com/watch?v=IR0UM33botU

Quelle: Socialmediaexplorer.com / www.youtube

❖.Bedrohungen: E-Mail & Web-Site Phishing Beispiele

Von ING DiBa <helpdesk@emaxxtelecom.com>
Betreff **ING DiBa - Telebanking PIN Aktualisierung**
An
Antworten | Weiterleiten | Junk | Lös
15.11.2014
Andere Aktion

Probleme diese E-Mail zu sehen? Im Browser anzeigen

ING DiBa
Die Bank und Du

ING DiBa Banking Login
führt zu
https://banking.ing-diba.de/ (OK)

Telebanking PIN
Aktualisierung

Unser Tipp: Jetzt online ausfüllen und Gebühren sparen!

Mit freundlichen Grüßen
ING DiBa

Sehr geehrte/r Kunde,

Unser System hat festgestellt, dass Ihr Telefon-Banking PIN aus Sicherheitsgründen geändert werden muss.

Von order-update@amazon.com <order-update@amazon.com>
Betreff **Amazon.com - Your Cancellation (7514-18152-7563029)**
An kaschemmenwirt@kaschemme.de
08.03.2

Dear Customer,

Your order has been successfully canceled. For your reference, here's a summary of your order:

You just canceled order #9854-7832289-86528

Klassische Phishing-Mail:

Von Facebook <notification+muikjvysyc@facebookmail.com>
Betreff **Facebook Support has sent you a message**
Antwort an noreply <noreply@facebookmail.com>
An [redacted].de

facebook

Facebook has sent you a message

To receive message, follow the link below:
http://www.facebook.com/support/message/muikjvysyc

Thanks,
The Facebook Support

See All Messages

The message was sent to [redacted].de. If you don't want to receive these emails from Facebook in the future or have your email address used for friend suggestions, you can unsubscribe. Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

Quelle: https://unsicherheitsblog.de/tag/phishing

❖.Bedrohungen: Brute-Force Angriff, wie sicher ist ein Passwort?

Maximale Rechenzeit eines Brute-Force-Angriffs bei 1 Milliarde Schlüsseln pro Sekunde

	Passwortlänge								
Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**	**11 Zeichen**	**12 Zeichen**
10 [0–9]	<1 ms	<1 ms	1 ms	10 ms	100 ms	1 Sekunde	10 Sekunden	2 Minuten	17 Minuten
26 [a–z]	<1 Sekunde	<1 Sekunde	<1 Sekunde	8 Sekunden	4 Minuten	2 Stunden	2 Tage	42 Tage	3 Jahre
52 [A–Z; a–z]	<1 Sekunde	<1 Sekunde	20 Sekunden	17 Minuten	15 Stunden	33 Tage	5 Jahre	238 Jahre	12.400 Jahre
62 [A–Z; a–z; 0–9]	<1 Sekunde	<1 Sekunde	58 Sekunden	1 Stunde	3 Tage	159 Tage	27 Jahre	1.649 Jahre	102.000 Jahre
96 (+Sonderzeichen)	<1 Sekunde	8 Sekunden	13 Minuten	21 Stunden	84 Tage	22 Jahre	2.108 Jahre	202.000 Jahre	19 Mio Jahre

Brute-Force-Angriffe versuchen, Passwörter mittels vielfacher Versuche zu ermitteln. Dabei werden sekündlich eine Vielzahl (bis zu 2 Billionen) an möglichen Passwörtern eingegeben, bis das richtige gefunden wird.

Quelle: Melani

❖.Bedrohungen: Skimming

https://www.youtube.com/watch?v=FtalA-URnoc

Quelle: https://krebsonsecurity.com/ / shuttlerstcck.com / Polizei

❖ .Bedrohungen: Rechtliches

- Der Schaden ist da, das Konto leer. Wer zahlt?
- Jedes Login basiert auf einem Vertrag
- Ein Blick in die AGB lohnt sich!
  Wer zahlt ist meistens unter «Mitwirkung und Sorgfaltspflichten des Kunden» definiert.

Tatbestände Cybercrime
- ✓ Unbefugte Datenbeschaffung
- ✓ Unbefugtes Eindringen in ein Datenverarbeitungssystem
- ✓ Datenbeschädigung
- ✓ Betrügerischer Missbrauch einer Datenverarbeitungsanlage
- ✓ Betrug

Quelle:

❖ .Bedrohungen: Anlaufstellen

Hauptseite:	https://www.melani.admin.ch/melani/de/home.html
Antiphishing:	https://www.antiphishing.ch/de/
Check:	https://www.checktool.ch
CyberPolice:	https://www.cybercrimepolice.ch/

Quelle: Melani / CyberPolice

❖.Bedrohungen:

Fragen?

Quelle:

❖.Sicherheit: Ein sicheres Passwort

https://www.youtube.com/watch?v=jtFc6B5lmIM

Quelle: https://www.datenschutz.org/sicheres-passwort

❖.Sicherheit: Ein sicheres Passwort

Ein absolut unknackbares Passwort gibt es nicht

Unsichere Passwörter:

hallo
1234
123456
password
passwort
hallo123
qwertz
arschloch
schatz
hallo1

Diese Google-Suche und Bing-Suche führen zu Listen von unsicheren Passwörter

Quelle: https://www.datenschutz.org/sicheres-passwort/

❖.Sicherheit: Aktuelle Regeln für ein sicheres Passwort

✓Wenig Sonderzeichen verwenden (<>/&%+“)	neu
✓Umlaute sollten vermieden werden (im Ausland keine Tastatur mit…)	bisher
✓Verwenden Sie Gross- / Kleinschreibung	bisher
✓Mischen Sie Buchstaben (Gross-/Klein) und Zahlen	bisher
✓Je länger umso besser (mind. 8 Zeichen)	neu
✓Für wichtige Passwörter (WLAN PW) sollte die Länge mind. 20 Zeichen sein	bisher
✓Verwenden Sie Phrasen (Sätze) anstatt kryptische Passwörter	neu
✓Keine einfachen Wörter verwenden. Ungeeignet sind der eigene Name, des Haustiers oder Verwandten, Geburtstage, Namen von Prominenten oder Städte	bisher
✓Keine Tastaturwiederholungen (1111111, qwertz..)	bisher
✓Keine simple Passwörter mit Sonderzeichen am Anfang / Ende (!Pizza)	bisher
✓Kein Recycling von Passwörter (1 pro Login mit mind. 4 Unterschiede zu anderen Passwörter).	bisher

Quelle: Internet

❖.Sicherheit: Beispiele für sichere manuell generierte Passwörter

- Man denkt sich einen Satz aus und setzt den 1. Buchstabe jedes Wortes in Grossbuchstaben. Man kann noch Zahlen oder Sonderzeichen hinzufügen.
  IchKaufeHeuteMorgen20Ruebli

- Man denkt sich einen Satz mit Bezug auf das Login und ergänzt es noch Zahlen oder Sonderzeichen hinzufügen.
  AmazonVerdientVielZuViel_+20%

- Man denkt sich einen Satz aus und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den zweiten oder letzten). Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen
  "Morgens stehe ich auf und putze mir meine Zähne drei Minuten lang."
  Nur die ersten Buchstaben: MsiaupmmZdMl
  "i und l" sieht aus wie "1", "&" ersetzt das "und": Ms1a&pmmZ3M1

Quelle: Internet

❖.Sicherheit: So kann man auch ein Passwort generieren

Wie ein Bayer sein Passwort wählt

Bitte geben Sie ein sicheres Passwort ein.
Leberkas
Entschuldigung, Ihr Passwort ist zu kurz!
Lerbkas-Semmel
Entschuldigung, Ihr Passwort muss mindestens eine Zahl enthalten.
1 Leberkas-Semmel
Entschuldigung, Ihr Passwort darf keine Leerzeichen enthalten.
50dreckskeberkassemmeln
Entschuldigung, Ihr Passwort muss mindestens einen Umlaut enthalten.
50dreckskeberkässemmelnzefix
Entschuldigung, Ihr Passwort muss mindestens 1 Großbuchstaben enthalten
50DRECKSleberkässemmelnZEFIX
Entschuldigung, Ihr Passwort muss mindestens 1 Sonderzeichen enthalten.
50DRECKSleberkässemmelnZEFIX!!!!!!
Entschuldigung, ihr Passwort darf nur Großbuchstaben enthalten, die nicht aufeinanderfolgend sind.
KreizKruzeFixVerdammterScheissDrecklatzkannstMiGleiKreizWeisSonstWo
WosIsnDesFiaAScheissSystem50DrecksleberkässemmelnZeFiX!!!!!!
Entschuldigung, dieses Passwort ist bereits in Verwendung. Bitte wählen sie ein anderes.

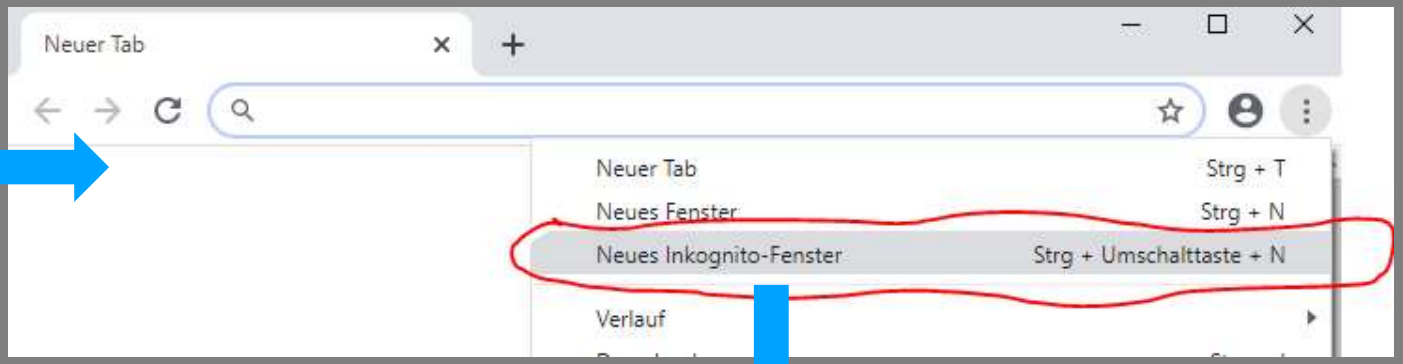
Quelle: Internet

❖.Sicherheit: Tipps rund um Passwörter

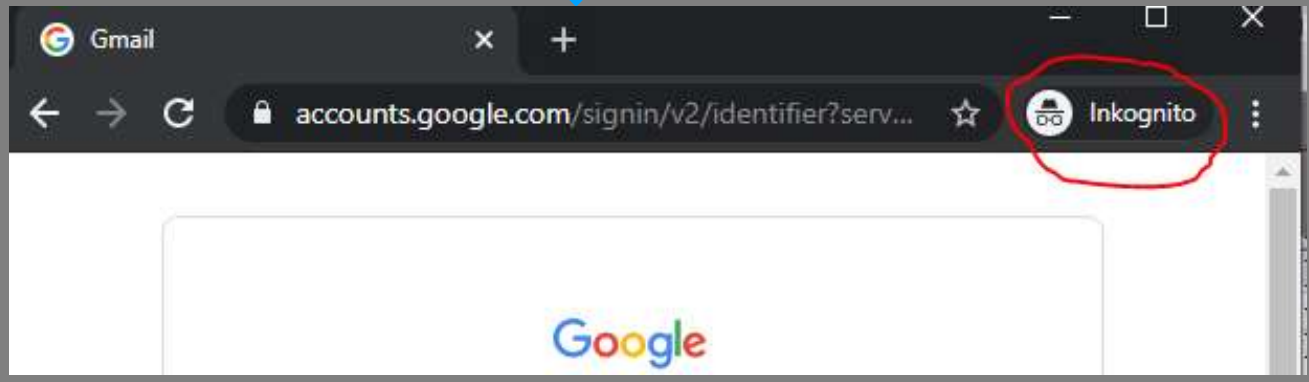
- ✓Nach Nutzung, sich immer abmelden, nicht Browser schliessen
- ✓Passwort nur bei Bedarf ändern neu
- ✓Keine Sicherheitsfragen mehr definieren neu
- ✓Wenn das Account nicht mehr benötigt wird, löschen lassen
- ✓Bei jedem neuen Account, sich die Frage stellen «Brauche ich eine Registrierung?» (neuerdings kann man als «Gast» kaufen)
- ✓Speicherung von Passwörter im Browser vermeiden oder restriktiv handhaben
- ✓Wenn möglich, Browser im «Private Modus» verwenden
- ✓Alle genutzten IT-Infrastruktur (Handy / PC / Tablet….) immer aktuell halten (OS, Virenscan, Programme…)
- ✓Die wichtigsten Passwörter (Windows / iOS / Android) sicher notieren und / oder die Methodik für die Wiederherstellung notieren.

Quelle:

❖.Sicherheit: Browser im „Private Modus“



"privates Fenster" bei Firefox,
"InPrivate-Fenster" bei Edge,
„Private Surfen“ im Safari

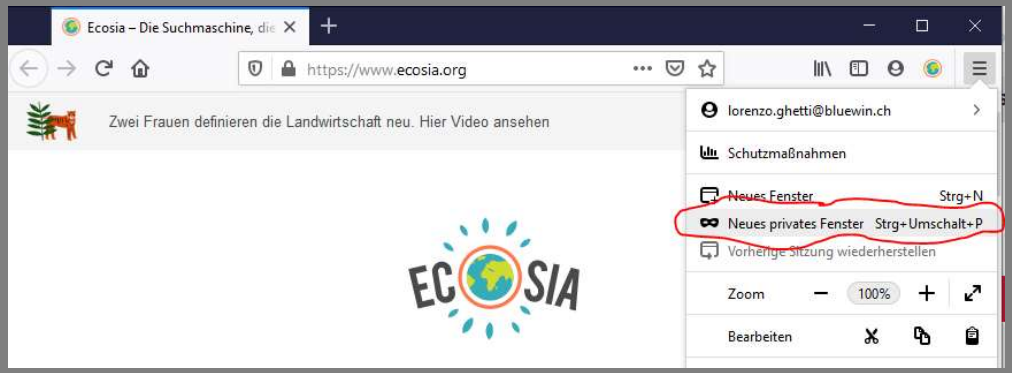


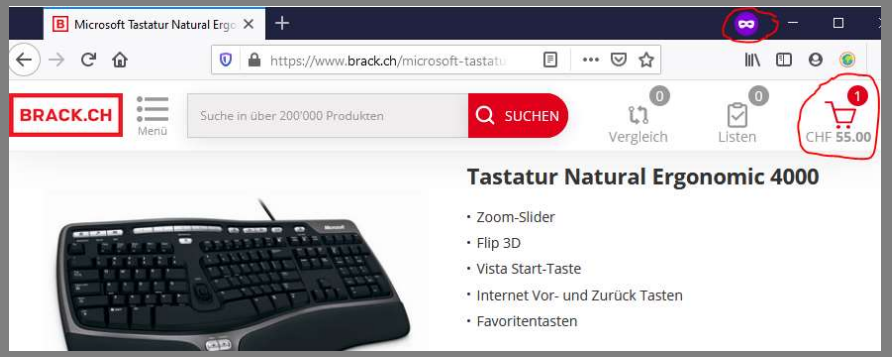
Es werden weniger / keine Spuren im Internet hinterlassen und im eigenen PC gespeichert

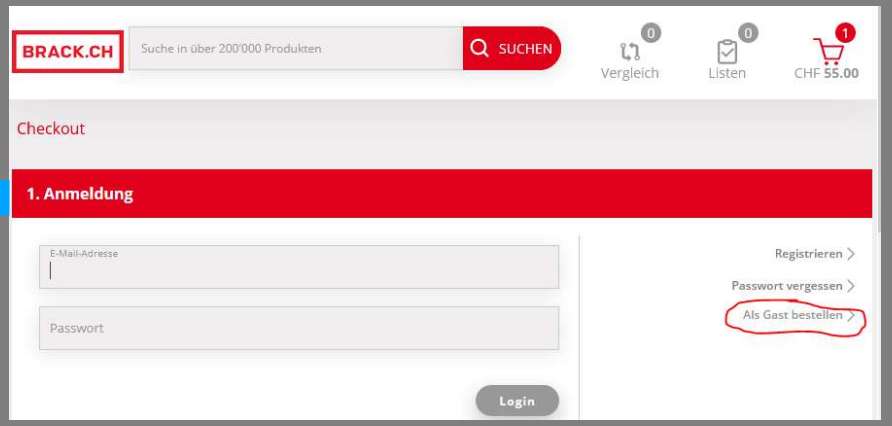
Quelle:

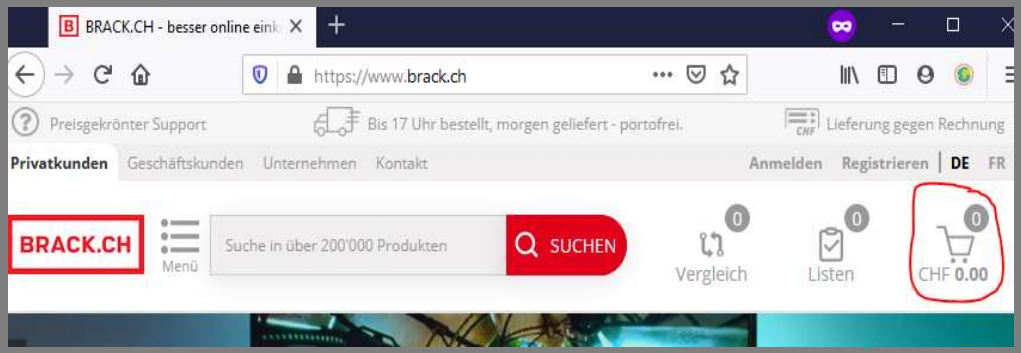
❖ .Sicherheit: „Kaufen als Gast“ mit einem „Private Browser“

Bei der Website BRACK als „Gast“ eine Tastatur kaufen









Quelle:

❖.Sicherheit:

Fragen?

❖.Sicherheit:

PAUSE

Quelle:

❖ .PW-Verwaltung: ZWECK

- Jeder PC Anwender muss durchschnittlich für seine Logins (Kreditkarte, PC-Login, Mobile Login, Online Banking, Social Media Logins, Online Shopping 29 Passwörter kennen.
- Die meisten können maximal 7 Passwörter / PIN im Kopf behalten
- 37% der Menschen vergessen mindestens ein Passwort wöchentlich

→ Passwort - Verwaltung

Quelle:

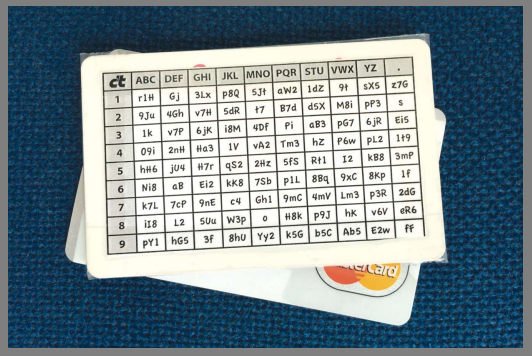
❖ .PW-Verwaltung: Methoden

Methodik

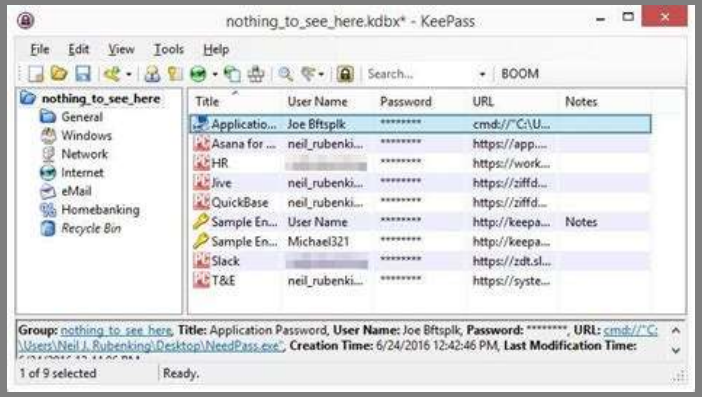
Papier

Browser

Oder eine Kombination der aufgeführten Methoden



Papier-Generator



PW Verwaltungsprogramm

Quelle: Internet

❖.PW-Verwaltung: Was muss notiert werden?

➢Datum der Erfassung	2020.02.14
➢Die Applikation / Webseite	https://www.digitec.ch/login
➢Der Username	hans.muster@switch.ch
Das Passwort selber	XXXXXXXXXXXXXXXXXXX
➢Optional: Kundennummer	ZH12345678-ZJ
➢Optional: Datum des letzten PW Wechsel	
➢Optional: Die Sicherheitsfrage	
➢Optional: Bemerkungen	Vorauszahlung

*minimal notwendig

Quelle: Internet

❖.PW-Verwaltung: Die Kopf-Methode

- Immer die gleiche Methode anwenden
  z.B. „Basis-PW“_„Name der Webseite“_“loginname“_“Sonderzeichen / Reihenfolge“
  Gnu34£1_Digitec_Bismark_12
- Oder
  Sätze mit Bezug auf die Applikation
  Bei_Digitec_Kann_Ich_Computer_kaufen

- Pro Login ein eigenes Passwort generieren

- Methodik niemandem bekannt geben, auch nicht als Beispiel oder Hilfe.

- Wenn die Methodik gewechselt wird, dann bei sämtlichen Login nachvollziehen.

Quelle: Internet

❖.PW-Verwaltung: Passwörter notieren

Es gibt verschiedene Methoden um Passwörter auf einem Papier zu notieren

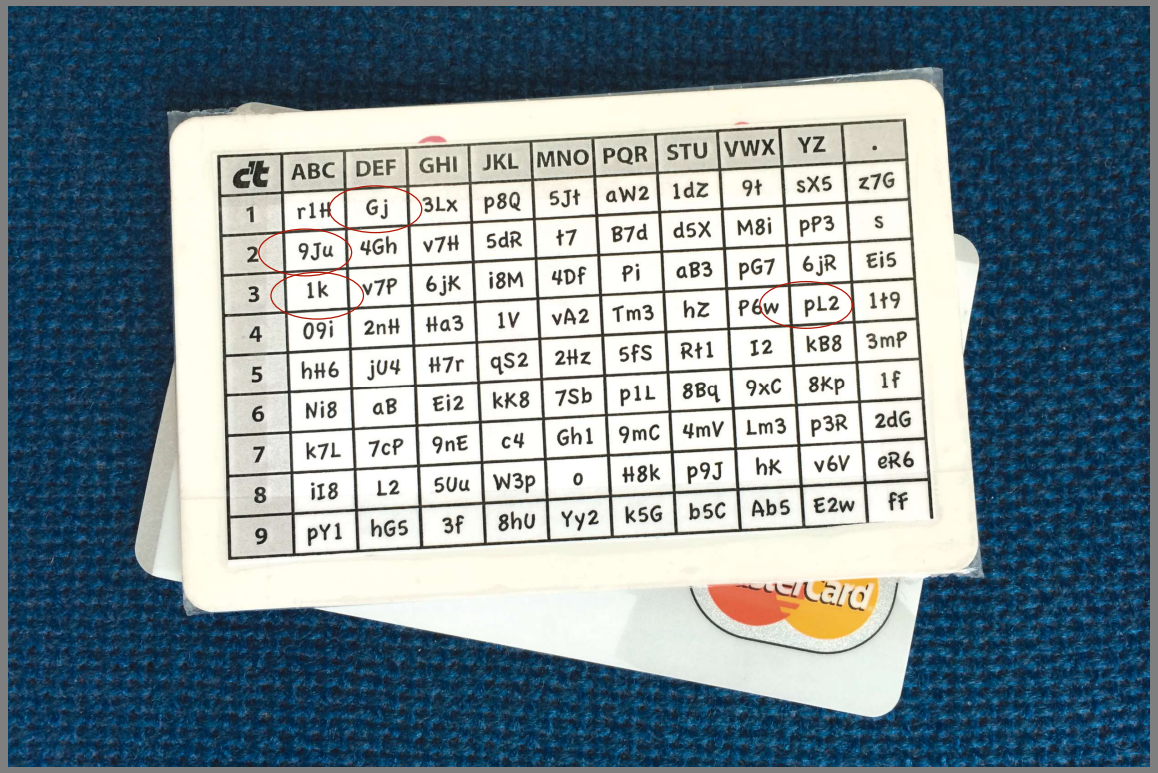
Häufig werden sie als Eintrag im Telefonbuch / Agenda „versteckt“.

Kann auch als Backup für die elektronisch verwalteten Passwörter verwendet werden.

NIE zusammen mit Kreditkarten oder andere Sicherheitselemente (z.B. Onlinebanking) ablegen

Quelle:

❖.PW-Verwaltung: Papier-Generator



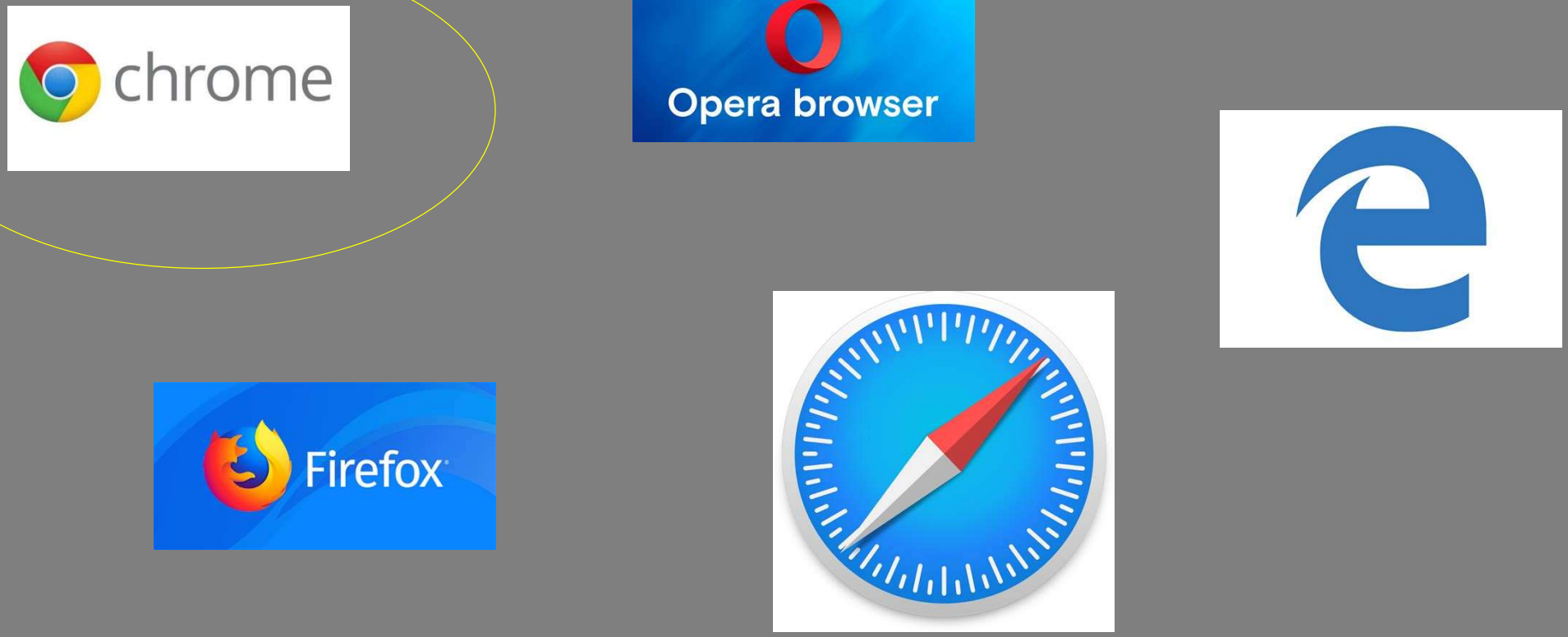
ct	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ	.
1	r1H	Gj	3Lx	p8Q	5Jt	aW2	1dZ	9t	sX5	z7G
2	9Ju	4Gh	v7H	5dR	t7	B7d	d5X	M8i	pP3	s
3	1k	v7P	6jK	i8M	4Df	Pi	aB3	pG7	6jR	Ei5
4	09i	2nH	Ha3	1V	vA2	Tm3	hZ	P6w	pL2	1t9
5	hH6	jU4	H7r	qS2	2Hz	5fS	Rt1	I2	kB8	3mP
6	Ni8	aB	Ei2	kK8	7Sb	p1L	8Bq	9xC	8Kp	1f
7	k7L	7cP	9nE	c4	Gh1	9mC	4mV	Lm3	p3R	2dG
8	iI8	L2	5Uu	W3p	o	H8k	p9J	hK	v6V	eR6
9	pY1	hG5	3f	8hU	Yy2	k5G	b5C	Ab5	E2w	ff

Ebay=Gj9Ju1kpL2

- Schreiben Sie in jedes Feld ein bis drei zufällige Zeichen, nach den bereits bekannten Regeln.
- Um ein Passwort für eine Site abzulesen, benutzen Sie einfach die Domain: Bei ebay.de lesen Sie beispielsweise in der ersten Tabellenzeile die Zeichenfolge unter E ab (1.Zeile), in der zweiten die unter B und so weiter.
- Bei langen Domains genügt es wahrscheinlich, wenn Sie die ersten fünf Buchstaben benutzen.

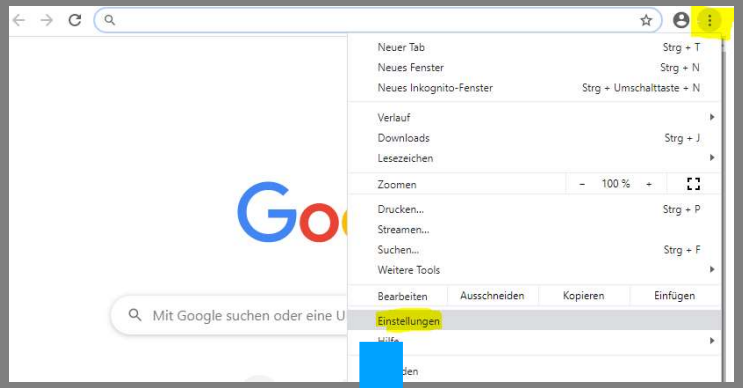
Quelle:https://www.heise.de/ct/ausgabe/2014-18-Kennwoerter-mit-Zettel-und-Stift-verwalten-2283904.html

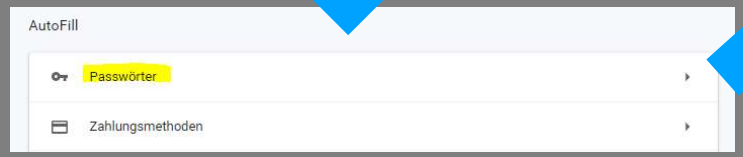
❖.PW-Verwaltung: Browser

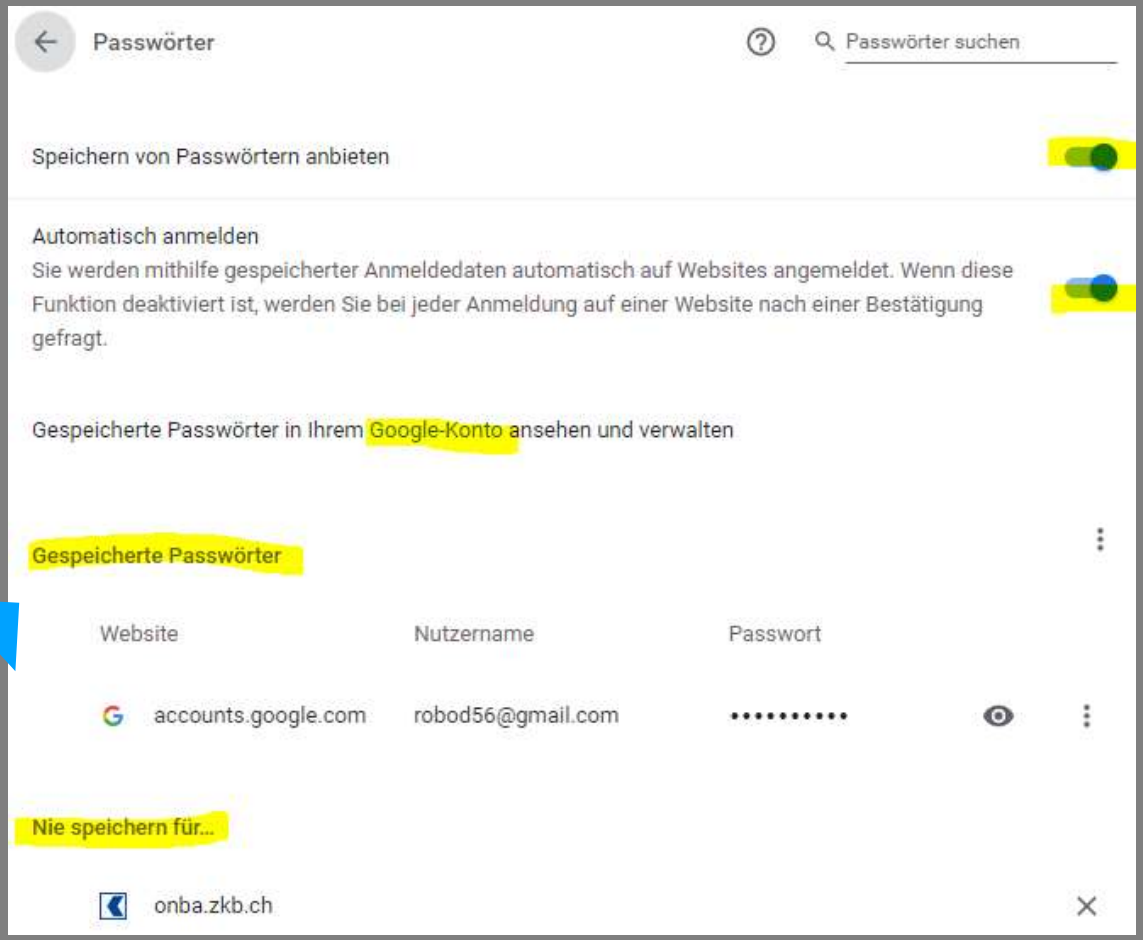


Quelle: Internet

❖.PW-Verwaltung: Browser Chrome







Quelle: Chrome

❖.PW-Verwaltung: Programme

Vorteile

>Passwort-Manager speichern Passwörter in verschlüsselten Datenbanken

>Eingebaute Passwort-Generatoren erzeugen sichere Passwörter

>Per Mausklick oder Fingertipp loggen sich Passwort-Manager automatisch für Nutzer ein

Nachteile

>Den Passwort-Diensten muss man Vertrauen entgegenbringen, sie synchronisieren die gespeicherten Passwörter automatisch.

>Bei vergessenem Masterpasswort sind sämtliche Kennwörter verloren

>Trotz Speicherschutz und Co sind Passwortmanager anfällig für Keylogger

Quelle:

❖.PW-Verwaltung: Die besten Programme 2019

Passwortmanager Überblick	1. Platz LastPass Premium	2. Platz 1Password	3. Platz Password Manager Pro	4. Platz KeePass	5. Platz Dashlane Premium	6. Platz Passwort Safe 7	7. Platz Bitwarden Password-Mgr.	8. Platz Password Manager
Gesamtwertung	1,1	1,2	1,4	1,4	1,4	2,3	2,5	2,9
Sicherheit (60 Prozent)	1,2	1,1	1,4	1,0	1,1	2,7	3,1	3,4
Bedienung (30 Prozent)	1,0	1,3	1,3	2,3	1,9	1,7	1,5	2,0
Ausstattung (10 Prozent)	1,1	1,0	1,9	1,9	2,4	2,2	1,9	1,8
Getestete Version	4.19.0	7.2.581	1.10.4.27461	2.40	6.1848.0	7.75.0	1.11.2	9.0.1.447
Hersteller	LogMeIn	Agile Bits	Avira	Dominik Reichl	Dashlane	ArchiCrypt	Bit Solutions LLC	Kaspersky Labs
Preis (ca.)	21 € pro Jahr	32 € pro Jahr	24,95 € pro Jahr	kostenlos	35 € pro Jahr	24,95 € Euro	kostenlos	13,95 € pro Jahr
SICHERHEIT								
Sicherheitskonzept/Verschlüsselung	Dienst/AES256	Dienst/AES256	Dienst/AES256	Lokal/AES256	Dienst/AES256	Lokal/AES256	Dienst/AES256	Dienst/AES256
Schutz vor einfachen Masterpasswörtern	●	●	●	○	●	○	○	●
Zusätzlicher Schutz für Masterpasswort /2-Faktor-Authentisierung	●/●	●/●	●/●	●/●	●/●	●/●	●/●	○/○
Sicherheits-Check für Passwörter/ Passwortdubletten aufspüren	●/●	●/●	●/●	●/●	●/●	nur einzeln/○	nur einzeln/○	●/●
Warnung bei Kontohacks	●	●	●	●	●	○	●	○
BEDIENUNG								
Installation nötig	○	○	○	○	●	○	○	●
Einrichtung/Bedienung Windows	sehr einfach/einfach	mittel/einfach	sehr einfach/einfach	mittel/mittel	einfach/mittel	mittel/einfach	mittel/einfach	mittel/mittel
Einrichtung/Bedienung Android	sehr einfach/sehr einfach	einfach/sehr einfach	einfach/sehr einfach	mittel/mittel	sehr einfach/sehr einfach	mittel/einfach	mittel/sehr einfach	mittel/einfach
Einrichtung/Bedienung iOS	sehr einfach/sehr einfach	einfach/sehr einfach	einfach/sehr einfach	mittel/mittel	sehr einfach/sehr einfach	mittel/einfach	mittel/sehr einfach	mittel/einfach
Log-In per Copy-and-Paste/Autofill	●/●	●/●	●/●	●/●	●/●	●/●	●/●	●/●
Datenbankabgleich mit anderen Geräten	automatisch	automatisch	automatisch	manuell	automatisch	manuell	automatisch	automatisch
AUSSTATTUNG								
Mehrere PW-Datenbanken/Ordnerstruktur	○/●	●/●	○/○	●/●	○/●	●/●	○/●	○/●
Passwortimport/export	●/●	●/●	●/●	●/●	●/●	●/●	●/●	●/●
Favoriten/Einträge kopieren	●/●	●/●	●/○	○/●	○/○	●/●	●/○	●/○
Passwortgenerator	gut	befriedigend	gut	gut	befriedigend	befriedigend	gut	befriedigend
Anzahl unterstützter Geräte	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	Einzelplatzlizenz**	unbegrenzt	unbegrenzt
Speichert Name/Benutzername/Passwort/Link	●/●/●/●	●/●/●/●	●/●/●/●	●/●/●/●	●/●/●/●	●/●/●/●	●/●/●/●	●/●/●/●
Speichert Notizen/Dateianhänge	●/●	●/●	●/○	●/●	●/○	●/●	●/○	●/○
Integration Chrome/Firefox	●/●	●/●	●/●	●/●	●/●	●/●	●/●	●/●

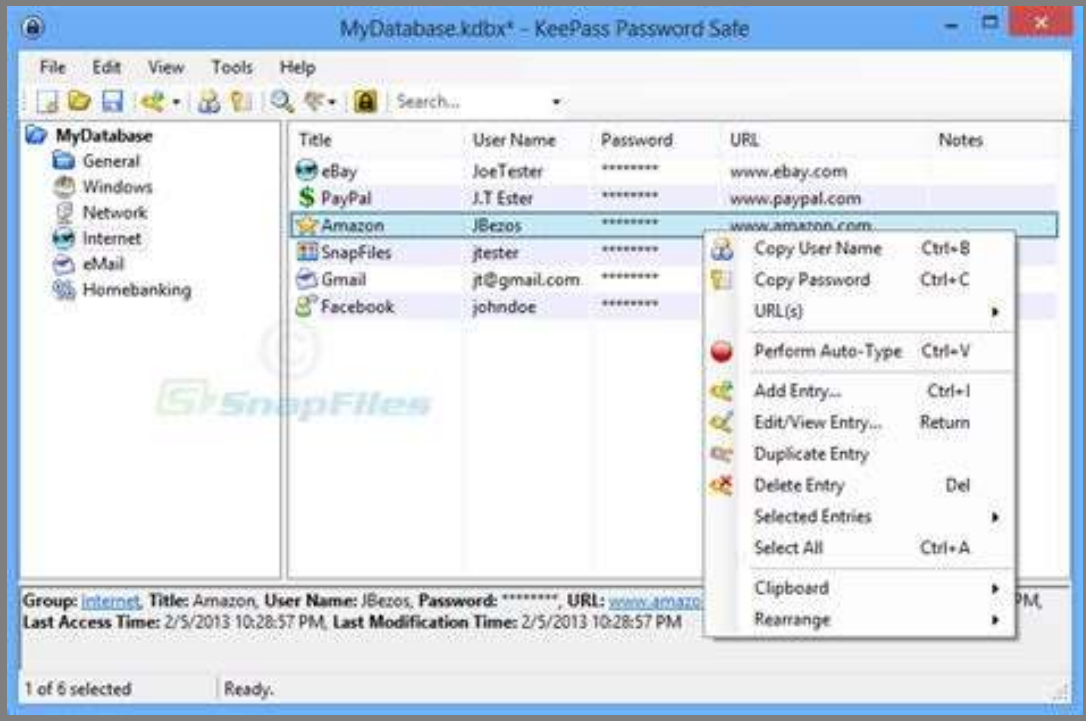
sehr gut (1–1,5) gut (1,6–2,5) befriedigend (2,6–3,5) ausreichend (3,6–4,5) mangelhaft (ab 4,6)
Alle Wertungen nach dem Schulnotensystem ● ja ○ nein

Test-Kandidaten: Das sind die besten Passwort-Manager 2019 CHIP

Quelle: Chip

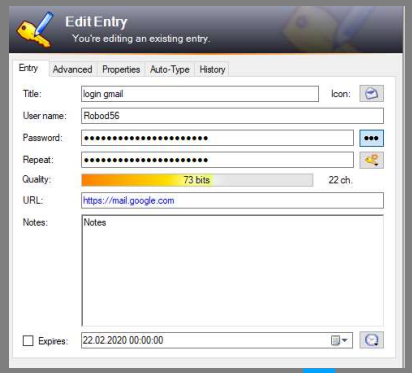
❖.PW-Verwaltung: Wichtige Funktionen (am Beispiel KeePass)

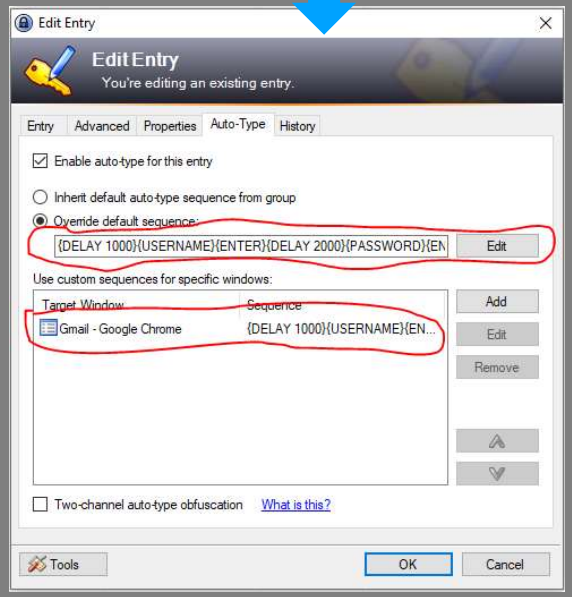
- ❖Installieren / Einrichten / updaten
- ❖Neuer Eintrag
- ❖Anzeige PW-Qualität
- ❖Anwenden (Username/PW)
- ❖Eintrag editieren
- ❖Eintrag löschen / Archivieren
- ❖Einträge gruppieren
- ❖Passwort generieren
- ❖Daten exportieren
- ❖PW Liste erstellen
- ❖Backup
- ❖Check ob gleiches Passwort verw. wurde

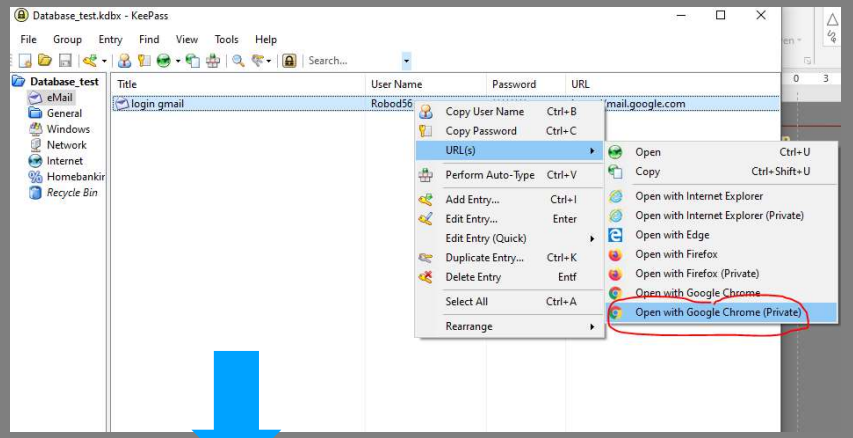


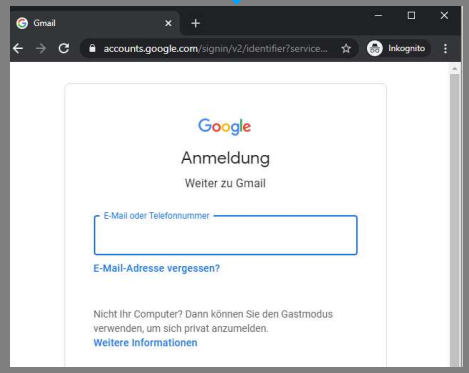
Quelle:

❖.PW-Verwaltung: Automatisches Login

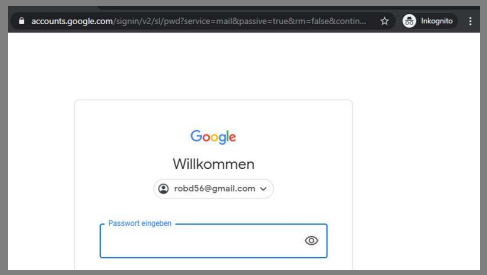








CTRL+ ALT+ A



Quelle:

❖.PW-Verwaltung: Sonderfälle

- ❖Master-PW vergessen
- ❖Daten korrupt
- ❖DB mit unterschiedliche Stände
- ❖Familie
- ❖Programm ersetzen
- ❖Programm auf mehreren PC (Sync)
- ❖Programm auf mehreren OS

Quelle:

❖.PW-Verwaltung:

Fragen?

❖.PW-Verwaltung:

VIELEN DANK

Fragen / Anregungen / Rückmeldungen

Computeria Wallisellen

https://www.computeria-wallisellen.ch/

info@computeria-wallisellen.ch

Quellennachweis / weiterführende Links

- https://100woerter.de/die-100-haeufigsten-passwoerter
- https://unsicherheitsblog.de/sicherheitsvorsorgeplan/passwoerter_kennwoerter
- https://unsicherheitsblog.de/tag/phishing
- https://www.antiphishing.ch/de/
- https://www.melani.admin.ch/melani/de/home.html
- https://krebsonsecurity.com/
- https://www.govcert.ch/statistics/
- https://sicheres-passwort-generator.de/
- https://www.google.de/search?&q=sex4me+rosebud+joshua+letmein+password
- https://sicheres-passwort-generator.de/passphrase.html
- Have I Been Pwned
- Mozilla's Firefox Monitor
- Google's Password Checkup
- https://www.heise.de/ct/ausgabe/2014-18-Kennwoerter-mit-Zettel-und-Stift-verwalten-2283904.html
- https://www.cybercrimepolice.ch/